DOCUMENT RESUME

ED 409 176 SE 060 323

AUTHOR	Rochowicz, John A., Jr.
TITLE	A Technological View of Modular Congruences.
PUB DATE	97
NOTE	16p.
PUB TYPE	Guides - Classroom - Teacher (052)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Elementary Secondary Education; *Mathematical Concepts; *Mathematics Activities; *Number Concepts; Spreadsheets; Teaching Guides; *Technology

ABSTRACT

Many students have difficulty finding remainders instead of quotients in the division of two numbers. Students are too quick to use technology and cannot interpret the output correctly. Moreover, many students are not accustomed to doing different yet applicable mathematics. As with all branches of mathematics, modular arithmetic and congruences are useful in real life situations. The use of technology allows students to focus on meanings and apply practice concepts. This paper describes various ways to compute modular congruences on a spreadsheet. Macros are discussed that provide the user with automatic computation of congruence. A drill for the practice of calculating congruences is also included. (Author/NB)

A Technological View of Modular Congruences

John A. Rochowicz, Jr

Alvernia College

Mathematics Department

Abstract

Many students have difficulty in finding remainders instead of quotients in the division of 2 numbers. They use technology too quickly and cannot interpret the output correctly. Also, many students are not accustomed to doing different yet applicable mathematics. As with all branches of mathematics, modular arithmetic and congruences are useful for relevant situations. The use of technology allows students to focus on meanings and apply and practice concepts. This paper describes various ways to compute modular congruences on a spreadsheet. Macros are discussed that provide the user with automatic computation of congruences. A drill for the practice of calculating congruences is also available.

Introduction

In many liberal arts mathematics courses, the meanings of quotient and remainder and their value for relevant mathematics are not understood by many students. Also, making connections between ideas and applications is difficult. The use of technology, computers or calculators automates many calculations and enables learners to apply mathematical concepts in more than one way.

Concepts associated with number theory and mathematical systems are important for mathematics learning and applications to everyday problem solving. From theoretical understanding to practical applications, modular arithmetic and congruences present students with the ability to do useful mathematics. The purpose of this paper is to show technological ways of calculating in different modular systems. Applications of congruences and a drill for congruence calculations are performed on a spreadsheet. Spreadsheets allow students to do mathematics as one does mathematics with pencil and paper. No black box effect exists and mathematics understanding of techniques and processes is more focused.

Congruences in the Classroom

When computers or calculators are applied to division, a decimal equivalent is provided. Lost is the meaning of a remainder when 2 numbers are divided. For example, with computer or calculator use, 66/15 results in output 4.4. From my liberal arts mathematics experiences, many students cannot find the remainder for 66/15 or interpret the output 4.4. They rely too much on technological output.

The concept of remainder when dividing 2 numbers is fundamental to many areas of mathematics. For any integers a and b and n an integer greater than one, a is congruent to b modulo n means that n divides a-b or a-b is divisible by n, and is symbolized by $a \equiv b \bmod n$. For

example, $33 \equiv 5 \bmod 4$ means 4 divides 33-5 or 4 divides 28. In the study of modular congruences the properties of closure, commutative, associative, identity, and inverse as related to congruences are usually taught. The operations of addition, subtraction, multiplication, and division in modular congruences are also discussed Conveying concepts already familiar to students but in different settings helps students acquire a general approach to learning mathematics. Technology use allows students various ways of calculating and applying modular arithmetic to many new situations.

Congruences and Spreadsheets

The computer can be used to determine when 2 numbers are congruent. By definition $a \equiv b \bmod n$ means n divides a-b for any integers a and b and n any integer greater than one. This definition can be implemented on a spreadsheet as a spreadsheet template or a macro.Table 1 displays the results of mod(42,9) or $42 \equiv x \bmod(9)$.

Insert Table 1 About Here

For Table 1, each cell does a specific job. In cell a2 enter a and in cell c2 enter the mod number b. In cell e2 enter a2 and in cell i2 enter c2. In cell g2 enter @int(+a2/c2). Using the cell formula e2-g2*i2 ouputs the correct result in b3. (The greatest integer for a2/c2 times c2 or i2 provides the amount to subtract from the first integer a in order to achieve the result). Line 4 can be added for concept reinforcement. In cell a4 enter a2, in e4 enter c2, and in cell c4 enter b3. Placing 42 in cell a2 and 9 in cell c2 automates the answer. Applying these cell formulas provides the user with automatic calculations of modular congruences.

For an easier technology tool for congruences, a spreadsheet macro is defined in Table 2. A macro is a sequence of commands that automate computations just as programming languages FORTRAN, BASIC or C do. In order to construct a macro in WINDOWS, place the cursor at the first command and use Tools Macro Run menus sequence. The macro then runs. Another way to make a macro is by using a macro button. Using the Tools Draw Button sequence of commands creates a button. This button asks for the range of values for the macro. The macro button can be named by typing the name in the text box. The Help menu in WINDOWS is a great aid in constructing macros. (See O'Leary & O'Leary, 1990 for making macros in DOS)

Insert Table 2 About Here

The macro in Table 2 automates the calculations of modular congruences. Each cell in column e has a specific task. Cell e1 erases cells a1 to d15. Cell e2 asks for an integer in cell b3 and in a3 waits for user response. Cell e3 asks for the mod and in cell a4 waits for user response.The value of a4 is placed in c6 and the word "is" is placed in cell a7. Cell e7 calculates the value of the congruence and places the result in cell b7.

Applying the built-in function @mod(a,b) also displays the remainder when a divides b. In the example, @mod(42,9) is 6.

An interesting way to find congruences is by applying the concept of left-sided or right-sided limits. A limit exists when a function becomes arbitrarily close to a number L as x approaches a value a from either side. That is, in mathematical notation $\lim_{x \to c} f(x) = L$

(Larson, Hostetler & Edwards, 1994, Finney & Thomas, 1990).

Table 3 calculates mod(a,b) in terms of left-sided limits defined by:

$$\lim_{x \to a^-} [b/2 - (b/pi)(atan(cot(pix/b)))]$$

Insert Table 3 About Here

Table 3 describes a macro for calculating congruences by applying limits. Cell e2 erases cells in the range a1 to d15. Then the macro asks for a, the value that x is approaching and waits for the user to respond in cell a3. Next the macro asks for the value of b in mod(a,b) and waits for the user to respond in cell a4. Cell e5 requests the user to enter the number of iterations desired for computing the limit and is placed in cell a5. The macro places the value for a5 in cell a6 for counting the number of iterations. Cell e8 starts a loop for finding the limit. Cells e9 and e10 use a sequence h (1/a6^10) that converges to 0. In cell b9 approaching from the left is entered and in cell a9, +a3-a7 (or a-h) is entered. Cell e13 requests the user to press ENTER key for each calculation. This macro then evaluates the limit in cells a10 and a11 and places the result in cell a11. For example, using mod(42,9) gives the correct result of 6.

Practical Uses and Applications

Finding the remainders when a number divides another number is a practical idea with many applications. Consider the example mod(42,9) or $42 \equiv x \bmod 9$. This means consider 42/9 or 9 divides 42 and find the remainder, not the result of the division. The result of mod(42,9) was found by using Table 1, Table 2, Table 3 and the built-in function @mod(a,b). (The result is 6 mod 9.)

Miller, Heeren, Hornsby (1994) and Smith (1984) provide numerous examples and applications requiring the use of congruences. The arithmetic and algebra of congruences and

applying congruences to practical situations are typical topics taught in liberal arts mathematics courses. In addition to these concepts, the ideas of a finite mathematical system with the properties of closure, commutative, associative, identity, and inverse are taught.

Implementation and Output of Congruences on a Spreadsheet

The types of examples I have used in my classes include:

1) Calculation: Many kinds of congruences can be analyzed. For example, determine the value for x in the congruence $199 \equiv x \bmod 6$ The result is 1 mod 6. Many examples of this type should be done without technology. As the user becomes more mentally proficient, any of the congruence methods defined in Table 1, Table 2, Table 3, or @mod(a,b) can be used to find the remainder when a number divides a second number.

2) Application: Many kinds of relevant problems are studied including dates, codes, and designs. For example, if today is Friday and my birthday is 151 days from today, on what day of the week is my birthday? Any congruence method will work from basic definition to limit definition to the built-in spreadsheet @mod(a,b) function. The result is found by considering congruences mod 7. The student has the opportunity to choose either method. Using 0 for Sunday, 1 for Monday and so forth, the day of the week for my birthday is found by calculating 151+5 mod 7 which is 2 or a Tuesday.

3 Drill: In order to have students focus on remainders instead of quotients and decimals when doing division, a macro drill is defined in Table 4. Practice and reinforcement permits students the opportunity to focus on remainders and not on technological output of decimal expressions

---

Insert Table 4 About Here

The drill macro allows the user to select the number of problems he or she wants. And a score is presented for the number of correct calculations reached

Each cell has a specific task to perform. Cell e3 erases the range of cells from a1 to d20. Cell e4 requests the user to enter the number of problems desired and cell e5 waits for a response in cell a3. A counter in a4 is defined in cell e6. In cell e7, the user is asked to enter the first integer and cell e8 waits for a response in cell a6. Cell e9 requests the user to enter the mod number and cell e10 waits for a response. Cell e11 asks the user to enter the answer in cell a10 and cell e12 waits for a user response. Cell e13 to cell e22 check the response of the user with the correct answer. If incorrect, the macro provides the correct answer. If correct, the macro calculates the number of problems correct and reports a percentage of correct out of the total number attempted

Classroom Experiences With Technology Use

In my liberal arts mathematics course, the meaning of an example such as, 75/4, is introduced without technology. After a variety of examples are studied without technology, a computer is used for alternative ways to calculate the quotient of 2 numbers. Quotient, remainder, and decimal equivalent are discussed. Mental calculations are performed and results are attained. For students who ask what good is this type of mathematics, applications are shown. Examples from casting out nines, chinese remainder theorem, coding and modular designs are explored beyond the basic arithmetic and algebra of congruences (Miller, Heeren, & Hornsby, 1994). Students think about solutions and then confirm solutions by calculating results in different ways. With any mathematics concepts, the value of its use is in practical applications. As students become better at calculating remainders when dividing 2 numbers, more applications and complex examples are considered.

The drill on congruence calculations helps students focus on the meanings of remainders. Table 4 displays a spreadsheet macro that drills students on finding congruences. Any desired number can be chosen and the macro grades the results of the drill. Through practice and repetition, concepts are reinforced and understood

Conclusion

The benefits of technology use are becoming clearer. Knowing when to use and when not to use technology for mathematics is necessary. Interpretation becomes an important aspect of learning. The student must learn to use technology effectively; its use without thought cannot be allowed. With the use of technology, learning in different ways is possible. Knowing ways of calculating modular congruences by definition, by built-in function @mod(a,b) and by limits gives students insights into alternative methods for successful solutions to applications. Motivation appears to increase with the use of technology. Topics in many areas such as number theory, calculus, and advanced matheamtics become unified with the study of modular congruences..

Despite using and developing software in different environments, the time and effort placed on applying technology to mathematics learning is worthwhile. I have constructed many LOTUS 1-2-3 for DOS spreadsheets and I have found that I can use these same spreadsheets in LOTUS 1-2-3 for WINDOWS with few modifications. The transition from DOS to WINDOWS was easy. The amount of time and energy placed on deveoping technological approaches to learning mathematics was not wasted. The use of technology for modular congruences provides learners with the capability to analyze and explore more complex problems without too much emphasis on techniques.

References

Arney, D.C. (1992). The Student Edition of DERIVE. Reading, MA: Addison-Wesley Publishing Company.

Finney, R.L.& Thomas, G. B. (1990). Calculus Reading, MA: Addison-Wesley Publishing Company.

Larson, R. E., Hostetler, R. P. & Edwards, B. H. (1994). Calculus With Analytic Geometry. (Fifth Edition). Lexington, MA:DC Heath and Company

Miller, C.D., Heeren, V.E., & Hornsby, E.J. (1994). Mathematical Ideas (7th ed.) New York, NY: Harper Collins College Publishers.

Niven, I. & Zuckerman, H. S. (1972). An Introduction to the Theory of Numbers. (3rd ed.)New York, NY: John Wiley & Sons, Inc.

O'Leary, T. J. & O'Leary L. I. (1990). The Student Edition of LOTUS 1-2-3 Release 2.2. Reading, MA: Addison-Wesley Publishing Company.

Smith, K.J (1984) The Nature of Mathematics.(4th ed.) Monterey, CA: Brooks/Cole Publishing Company.

Table 1.

Finding Congruences by Definition

	A	B	C	D	E	F	G	H	I
1	By definition:								
2	42	= x mod	9	means	42	-	4	*	9
3	=	6							
4	42	=	6	mod	9				

Note. The result is also found by using @mod(42,9).

Table 2

Finding Congruences by Macro

	A	B	E	F
1			/real.d15~	
2			{goto}b3~integer~{goto}a3~{?}~	
3			{goto}b4~Enter mod m~{goto}a4~{?}~	
4			{goto}a6~+a3~{goto}b6~ mod~	
5			{goto}c6~+a4~	
6			{goto}a7~is~	
7			{let b7,+a3-@int(a3/a4)*a4}~	

Note. In cell e7 using {let b7, @mod(a3,a4)}~ accomplishes the same result.

Table 3

Finding Congruences by Limits

	A	B	E	F
2			/real.d15~	
3			{goto}b3~Enter a~{goto}a3~{?}~	
4			{goto}b4~Enter b~{goto}a4~{?}~	
5			{goto}b5~Enter the number of terms desired~	
6			{goto}a5~{?}~	
7			{goto}a6~+a5~	
8			{for a6,1,(a6-1),1,e9}~	
9			{goto}b7~ = h ~	
10			{let a7,1/a6^10}~	
11			{goto}b9~approaching from left~	
12			{goto}a9~+a3-a7~	
13			{goto}b11~Press ENTER for each calculation~	
14			{let a10,+a4/2}	
15			{let a11,+a10-(+a4/@pi)*(@atan(@cot(@pi*+a9/+a4))) }~	
16			{goto}a11~{?}~	

Note. Congruences can be found by calcualting right-sided limits also.Arney (1992) defines mod(a,b) in terms of right-sided limits. The macro can be entered anywhere on the spreadsheet to allow room for documentation and output.

Table 4

A Macro Drill for Modular Congruences

	A	B	E	F
3			/real.d20~	
4			{goto}b3~Enter the number of problems~	
5			{goto}a3~{?}~	
6			{let a4,+a4+1}~	
7			{goto}b6~Enter the first integer~	
8			{goto}a6~{?}~	
9			{goto}b8~Enter the mod number~	
10			{goto}a8~{?}~	
11			{goto}b10~Enter the answer~	
12			{goto}a10~{?}~	
13			{if a10=@mod(a6,a8)}{branch e19}	
14			{goto}b12~The answer is incorrect~	
15			{goto}b14~is the correct answer~	
16			{let a14,@mod(a6,a8)}~	
17			{if a4<a3}{branch e6}~	
18				
19			/real2.d14~	
20			{let a18,a18+1}~{goto}b18~correct~	

Table 4 continued.

21	{let a20,(a18/a3)*100}~{goto}b20~percent right~
22	{if a4<a3}{branch e6}~

Note. The macro can be entered anywhere on the spreadsheet to allow room for documentation and output

SE060323

U.S. DEPARTMENT OF EDUCATION

EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

REPRODUCTION RELEASE

I. DOCUMENT IDENTIFICATION

Title: A Technological View of Modular Congruences

Author(s): John A. Rochowicz, JR

Date: 6/6/97

II. REPRODUCTION RELEASE

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, or electronic/optical media, and are sold through the ERIC Document Reproduction Service (EDRS) or other ERIC vendors. Credit is given to the source of each document. If reproduction release is granted, one of the following notices is affixed to the document.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY ____ TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)"	"PERMISSION TO REPRODUCE THIS MATERIAL IN **OTHER THAN PAPER COPY** HAS BEEN GRANTED BY ____ TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)"

If permission is granted to reproduce the identified document, please CHECK ONE of the options below and sign the release on the other side.

☒ Permitting microfiche (4" x 6" film) paper copy, electronic, and optical media reproduction (Level 1)

OR

☐ Permitting reproduction in other than paper copy (Level 2)

Documents will be processed as indicated, provided quality permits. If permission to reproduce is granted, but neither box is checked, documents will be processed at Level 1.

OVER

Detach and complete this form and submit with your document.

Signature Required

"I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce this document as indicated on the other side. Reproduction from the ERIC microfiche or electronic/optical media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries."

Signature: John A. Rochowicz Jr

Printed Name: John A. Rochowicz JR

Organization: Alvernia College

Position: Associate Prof of Mathematics

Address: 400 St. Bernardine Street Reading, PA

Tel. No: (610) 7968257 Zip Code: 19607

III. DOCUMENT AVAILABILITY INFORMATION

(Non-ERIC Source)

If permission to reproduce is not granted to ERIC, or, if you wish ERIC to cite the availability of the document from another source, please provide the following information regarding the availability of the document. (ERIC will not announce a document unless it is publicly available, and a dependable source can be specified. Contributors should also be aware that ERIC selection criteria are significantly more stringent for documents which cannot be made available through EDRS).

Publisher/Distributor: ____

Address: ____

Price Per Copy: ____

Quantity Price: ____

IV. REFERRAL TO COPYRIGHT/ REPRODUCTION RIGHTS HOLDER

If the right to grant reproduction release is held by someone other than the addressee, please provide the appropriate name and address: